CLAIMS

1. An apparatus for segregating traffic amongst a plurality of stations that are associated with an access point, comprising:

a LAN segment; and

a personal virtual bridged local area network (personal VLAN) for partitioning said LAN segment logically into multiple virtual bridged local area networks (VLANs).

2. The apparatus of Claim 1, said personal VLAN further comprising:

a VLAN bridge for forwarding unicast and group frames only to those ports that serve the VLAN to which the frames belong.

3. The apparatus of Claim 1, said personal VLAN further comprising:

a protocol for VLAN discovery.

4. The apparatus of Claim 1, said personal VLAN further comprising:

means for allowing a station to create a new port that serves a new VLAN, or to join an existing VLAN via an authentication protocol.

5. The apparatus of Claim 1, said personal VLAN further comprising:

one or more logical ports in which a Personal VLAN bridge can maintain more than one logical port per physical port, and bridges between ports of any kind.

6. The apparatus of Claim 1, said personal VLAN further comprising:

means for cryptographic VLAN separation in which in a Personal VLAN, a logical port serves at most one VLAN but, because there may be more than one logical port per physical port, more than one VLAN may exist on a physical port.

7. The apparatus of Claim 1, wherein traffic within one VLAN is separated from another VLAN on a same physical port by cryptography.

8. The apparatus of Claim 1, wherein an authentication code uniquely identifies a VLAN to which traffic belongs, while another level of encryption keeps traffic private except to members of said VLAN.

9. The apparatus of Claim 1, said personal VLAN further comprising:

an extended protocol comprising the IEEE 802.1Q-1998 (Virtual Bridged LANs) protocol.

10. The apparatus of Claim 1, further comprising:

means for providing layer-2 VLAN support across routers.

11. The apparatus of Claim 1, further comprising:

means for implementing a spanning tree algorithm when a personal VLAN permits an STA to create a VLAN where the STA itself is a bridge.

12. A method for segregating traffic amongst a plurality of stations that are associated with an access point, comprising the steps of:

providing a distribution system comprising multiple virtual local area networks (VLANs), wherein every station that associates with said access point can create a new VLAN with itself and said distribution system as its members, wherein a creator of a new VLAN can authenticate stations that wish to join said new VLAN; and

separating traffic between trusted and untrusted stations even though they associate with a same access point.

13. The method of Claim 12, further comprising the step of:

discovering existing VLANs.

14. The method of Claim 12, further comprising the step of:

joining an existing VLAN.

15. A method for segregating traffic amongst a plurality of stations that are associated with an access point, comprising the steps of:

providing a protocol for virtual local area network (VLAN) discovery;

allowing a station to create a new port that serves a new VLAN, or to join an existing VLAN.

maintaining more than one logical port per physical port; and

providing cryptographic VLAN separation, wherein traffic within one VLAN is separated from another VLAN on a same physical port by cryptography.

16. The method of Claim 15, further comprising the step of:

providing an authentication code that uniquely identifies a VLAN to which traffic belongs.

17. The method of Claim 16, further comprising the step of:

providing an encryption mechanism for keeping traffic private except to members of said VLAN.

18. The method of Claim 15, further comprising the step of:

providing for every port a personal VLAN control channel for sending and receiving control frames and authentication protocol frames.

19. In a system for segregating traffic amongst a plurality of stations that are associated with an access point, an apparatus for virtual local area network (VLAN) discovery, comprising:

a personal VLAN bridge for partitioning a LAN segment logically into multiple VLANs; and

server and client VLAN discovery agents associated with said VLAN bridge for discovering other VLANs and/or allowing VLANs that said VLAN bridge serves to be discovered.

20. The apparatus of Claim 19, further comprising:

means for transmitting a discover frame.

21. The apparatus of Claim 20, further comprising:

in response, means for transmitting a VLAN-OFFER frame to a source MAC address of said discover frame;

wherein said offer frame lists at least some of the VLANs served by a bridge and information that can be used to select from among them.

22. The apparatus of Claim 19, further comprising:

means for receiving a request to serve a new VLAN.

23. The apparatus of Claim 22, wherein said request contains a virtual LAN ID (VID) of a new VLAN.

24. In a system for segregating traffic amongst a plurality of stations that are associated with an access point, a method for requesting service for a new virtual local area network (VLAN), comprising the steps of:

a bridge receiving a request frame with a source MAC address through a control channel of a physical port, wherein a holder of said MAC address is a requester;

receiving said request frame initiating an authentication protocol with said requester through said control channel;

discarding said request if said requester cannot be authenticated, or is not authorized to request VLAN service from said bridge;

creating a new logical port and associating said new logical port with a physical port through which said request frame is received if there is no conflict in using a virtual LAN ID (VID) requested;

otherwise, said bridge negotiating a VID with said requester; and

updating port state information for said logical port to include a security association, shared with said requester, that is in effect for all traffic through said port .

25. In a system for segregating traffic amongst a plurality of stations that are associated with an access point, a method for linking a new virtual local area network (VLAN) to one or more existing VLANs served by physical ports of a bridge, comprising the steps of:

sending a join-VLAN request over a control channel;

authenticating said request wherein, if authentication fails, said request is discarded;

adding a logical port that serves a source VLAN to a member set of every virtual LAN ID (VID) in a set of VIDs for VLANs served by a set of physical ports which comprise destination VLANs; and

adding every physical port in said set of physical ports to a member set of said source VLAN;

and forming an untagged set of said source VLAN by taking a union of all untagged sets for VIDs in said set of VIDs for VLANs served by a set of physical ports which comprise destination VLANs;

wherein if a request frame contains a null VID in its tag header, or it is untagged, then a logical port of said bridge is added to an untagged set of every VID in set of VIDs for VLANs served by a set of physical ports which comprise destination VLANs.

26. In a system for segregating traffic amongst a plurality of stations that are associated with an access point, a method for joining a personal virtual local area network (VLAN) served by a logical port, comprising the steps of:

if source and destination VLANs have a same creator, and said creator issued a join-VLAN request, then said request is discarded;

if said source and destination VLANs are identical and said creator did not issue said request, then said creator authenticates said requester for membership into said personal VLAN; and

in all other cases, a bridge first authenticates said request to make sure that said requester is the creator of said source VLAN;

wherein if authentication succeeds, then said creator authenticates said requester for membership into said destination VLAN; and

wherein said requester authenticated said creator to make sure that said creator is the creator of said destination VLAN.

27. In a system for segregating traffic amongst a plurality of stations that are associated with an access point, a method for authenticating a request for joining a personal virtual local area network (VLAN) served by a logical port, comprising the steps of:

providing a personal VLAN bridge having a control channel for authentication of a requester by a creator;

said personal VLAN bridge using said control channel to relay authentication protocol messages between said creator and said requester; and

if said creator can authenticate said requester, then said creator sharing a security association it holds with said personal VLAN bridge with said requester as well.

28. The method of Claim 27, further comprising the step of:

providing ingress filtering at logical ports.

29. The method of Claim 27, wherein said security association contains at least two keys, one key for encryption and another key for computing an authentication code, wherein said security association is associated with a VLAN, wherein said authentication code is used to limit traffic at a logical port to members of an entire VLAN, wherein encryption is used to keep traffic private except to members, wherein only stations having said security association belong to said VLAN, and wherein all stations having said security association belong to the same broadcast domain.

30. The method of Claim 28, wherein a physical port may serve more than one VLAN by having multiple logical ports associated with it.

31. The method of Claim 27, further comprising the steps of:

if a received frame carries a null virtual LAN ID (VID) or is untagged, then using its source MAC address to determine a preliminary VLAN classification of a logical port;

if said frame carries a VID, then using said VID as said preliminary classification instead;

using said preliminary classification to index into a table of security associations giving an authentication code key;

said received frame carrying an authentication code computed over a frame payload using a message digest algorithm agreed upon by both said personal VLAN bridge and said requester at authentication time and having been recorded in said security association;

said personal VLAN bridge re-computing said authentication code, using said authentication code as an authentication code key, over said payload of said received frame;

comparing said re-computed authentication code with said received authentication code;

wherein if said re-computed authentication code and said received authentication code match, then said preliminary VLAN classification becomes a final VLAN classification;

using said final classification as a value of a VLAN classification parameter of any corresponding data request primitives;

decrypting said frame using said security association; and

submitting said decrypted frame to a forwarding and learning process;

otherwise, discarding said frame.

32. The method of Claim 27, wherein if a transmission port for a frame that belongs to a VLAN is not in a member set of said VLAN, then said frame is discarded.

33. An apparatus for segregating traffic amongst stations (STAs) that are associated with a bridge, comprising:

a personal virtual bridged local area network (personal VLAN) that uses a VLAN to segregate traffic.

34. The apparatus of Claim 33 said personal VLAN further comprising:

means associated with said personal VLAN for partitioning a LAN segment logically into multiple VLANs; and

a personal VLAN bridge associated with said personal VLAN for forwarding unicast and group frames only to those ports that serve a VLAN to which said frames belong.

35. The apparatus of Claim 34, wherein said personal VLAN bridge extends a standard VLAN bridge in at least any of the following ways:

VLAN discovery in which a personal VLAN bridge provides a protocol for VLAN discovery;

VLAN extension in which a personal VLAN allows a station to create a new port that serves a new VLAN, or to join an existing VLAN via an authentication protocol;

logical ports in which a personal VLAN bridge maintains more than one logical port per physical port, and bridges between ports of any kind; and

cryptographic VLAN separation in which in a personal VLAN, a logical port serves at most one VLAN but, because there may be more than one logical port per physical port, more than one VLAN may exist on a physical port.

36. The apparatus of Claim 35, wherein traffic within one VLAN is separated from another VLAN on a same physical port by cryptography.

37. The apparatus of Claim 35, wherein an authentication code uniquely identifies a VLAN to which said traffic belongs, while another level of encryption keeps traffic private except to members of said VLAN.